Application/Control Number 09/775,942

Art Unit: 2137

Claims Amendment

I claim:

1. (currently amended)

~~A method of securing communication, where~~

~~messages are passed between communicating parties encrypted with a one-time pad, for example by combining bits of a message and bits of the one-time pad using a logical XOR operation, through one channel or a group of channels,~~

~~the one-time pad is exchanged between communicating parties through another channel or a group of channels in an encrypted form with the use of private key encryption, for example DES~~.

A method of securing communication using two channels of communication, where

messages are exchanged between communicating parties encrypted with a one-time pad through one channel,

the one-time pad is exchanged between communicating parties in an encrypted form with the use of private key encryption through another channel,

the one-time pad is generated by communicating parties in pieces and exchanged between communicating parties in pieces in separate threads of execution concurrently with exchange of messages and other processing,

the estimate of the size of a next piece of one-time pad to be generated and exchanged is passed to these separate threads of execution in advance of message exchange and a ready piece of one time-pad is received from these threads, when needed to encrypt or decrypt a message.

2. (currently amended)
~~The method of securing communication of the claim 1, where the one-time pad is generated and passed between communicating parties concurrently with the rest of an application, which uses this secure communication.~~
The method of securing communication of the claim 1, where pieces of the one-time pad are dedicated either to encrypting messages sent in one direction or to encrypting messages sent in the opposite direction.

3. (original) The method of securing communication of the claim 1, where one-time pad is entirely generated by one communicating party and used by other communicating parties, and possibly by this one also.

4. (currently amended)
~~The method of securing communication of the claim 1, where the one-time pad consists of two or more parts, each part is generated by a different communicating party and parts are exchanged between communicating parties in an encrypted form.~~
The method of securing communication of the claim 1, where there are three communicating parties and the one-time pad is entirely generated by one of them.

5. (currently amended)

~~The method of securing communication of the claim 1, where a part of one-time pad is broken into a sequence of pieces and passed between communicating parties in pieces.~~

The method of securing communication of the claim 2, where pieces of the one-time pad used to encrypt messages sent in one direction are generated by one party and pieces of the one-time pad used to encrypt messages sent in the opposite direction are generated by another party.

6. (currently amended)

~~The method of securing communication of the claim 5, where the additional pieces of one-time pad are generated and passed between communicating parties as needed.~~

The method of securing communication of the claim 1, where encrypted exchange of the one-time pad is done using Secure Socket Layer protocol.

Alexander Liss 11/08/2004